

特集2

LSIを“盗聴”から守る

暗号回路へのサイドチャネル攻撃とその対策

デバイスの記事

本特集では，正規の通信経路（I/O ピン）以外からLSIの秘密情報（例えば暗号の秘密かぎ）を取り出す「サイドチャネル攻撃」を取り上げます．サイドチャネル攻撃は，例えば，LSIの動作時にチップそのものが発する電磁波や熱，消費電力の変化を解析して，データを読み取ります．特集では，サイドチャネル攻撃のからくりを押さえつつ，DES（Data Encryption Standard）やRSA，AES（Advanced Encryption Standard）などの暗号回路について，どのように対策を施すべきかその指針を述べます．